LUKAS, NACE, GUTIERREZ & SACHS

CHARTERED

1650 TYSONS BOULEVARD, SUITE 1500
MCLEAN, VIRGINIA 22102
703 584 8678 • 703 584 8696 FAX

WWW FCCLAW.COM

RUSSELL D. LUKAS
DAVID L. NACE
THOMAS GUTIERREZ*
ELIZABETH R. SACHS*
GEORGE L. LYON, JR.
PAMELA L. GIST
DAVID A. LAFURIA
TODD SLAMOWITZ*
B. LYNN F. RATNAVALE*
STEVEN M. CHERNOFF*
KATHERINE PATSAS*

CONSULTING ENGINEERS
ALI KUZEHKANANI
LEILA REZANAVAZ

OF COUNSEL
LEONARD S. KOLSKY*
JOHN CIMKO*
J. K. HAGE III*
JOHN J. MCAVOY*
HON. GERALD S. MCGOWAN*
TAMARA DAVIS-BROWN*

*NOT ADMITTED IN VA

Writer's Direct Dial
(703) 584-8665
pgist@fcclaw.com

February 28, 2008

Marlene H. Dortch, Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

Re: **EB Docket No. 06-36**
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2007

East Kentucky Network, LLC d/b/a Appalachian Wireless
Form 499 Filer ID 802104

Dear Ms. Dortch:

On behalf of East Kentucky Network, LLC d/b/a Appalachian Wireless, and pursuant to Section 64.2009(e) of FCC rules, there is submitted herewith the carriers' 2007 CPNI certification with accompanying statement. The documents are submitted in accordance with the directives set forth in the FCC's *Public Notice*, DA 08-171, EB Docket No. 06-36, released January 29, 2008.

Should any questions arise regarding this submission, please contact the undersigned.

Very truly yours,

Pamela L. Gist

Pamela L. Gist

Enclosures
cc: Enforcement Bureau, FCC (2)
Best Copy and Printing, Inc. (1)

EAST KENTUCKY NETWORK
101 TECHNOLOGY TRAIL
IVEL, KY 41642
PHONE: (606) 874-2550
FAX: (606) 874-7251
EMAIL: INFO@EKN.COM
WEBSITE: WWW.EKN.COM

EAST KENTUCKY NETWORK

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Annual 47 C F R § 64.2009(e) CPNI Certification for 2007

Company Name: East Kentucky Network, LLC
d/b/a Appalachian Wireless

Form 499 Filer ID: 802104

Address: 101 Technology Trail
Ivel, Kentucky 41642

CERTIFICATION

I, Gerald F Robinette, hereby certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures effective during the calendar year 2007 that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement that (i) explains how the company's procedures ensure that the company is in compliance with the requirements set forth in 47 C.F.R. §§ 64.2001 *et seq* of the rules, (ii) explains any actions taken against data brokers during the past year, (iii) reports information known to the company regarding tactics pretexters may be using to attempt access to CPNI, and (iv) summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI

Name: Gerald F. Robinette
Title: Chief Executive Officer
Date: February 28, 2008

2007 STATEMENT

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Company Name: East Kentucky Network, LLC
d/b/a Appalachian Wireless

Form 499 Filer ID: 802104

Address: 101 Technology Trail
Ivel, Kentucky 41642

STATEMENT

East Kentucky Network, LLC d/b/a Appalachian Wireless ("Carrier") has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI")

- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.

- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.

- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.

- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI. A process ensures that opt-out elections are recorded and followed

- Carrier has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise, and in connection with these procedures, Carrier has established a system of passwords and back-up authentication methods which complies with the requirements of applicable Commission rules.

- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.

- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.

- Carrier took no following actions against data brokers in 2007, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission

- Carrier has found that pretexters are attempting to access CPNI through phone calls and customer impersonation. Carrier's use of a passcode to properly authenticate customers, plus additional verification procedures, protects CPNI.

- Carrier received no customer complaints in 2007 regarding the unauthorized release of CPNI in any category (improper access by employees, improper disclosure to individuals not authorized to receive the information, improper access to online information by individuals not authorized to view the information, or other instances of improper access or disclosure.